What is claimed is:

1. A method for providing a time stamp by means of a tamper-proof time signal (5, 10) via a telecommunications network (2),
wherein a network user (1a, 1b, ..., 1e) requests an, in particular, officially recognized time signal (5, 10) from an, in particular, certified central system (3); said time signal being encrypted by the central system (3) with at least one key, transmitted to the network user (1a, 1b, ..., 1e) via the telecommunications network (2) after encryption, and decrypted by this network user with the same key or keys.

2. The method as recited in Claim 1,
wherein at least one key, which is present at both the network user (1a, 1b, ..., 1 e) and at a central system (3), changes synchronously at the network user and at the central system, especially after predetermined time intervals.

3. The method as recited in one of the preceding claims,
wherein the network user (1a, 1b, ..., 1e) and the central system (3) are each provided with at least one clock system (4a, 4b, ..., 4e, 6a, 6b, ..., 6e); each two of these clock systems (4a - 6a, 4b - 6b, ..., 4e - 6e) being assigned to each other and to the network user (1a, 1b, ...,1e) and operating synchronously to generate a key which changes synchronously in time.

4. The method as recited in one of the preceding claims,
wherein when a network user (1a, 1b, ..., 1e) requests a time signal (5, 10), the central system (3) determines a clock system (4a, 4b, ..., 4e) assigned to this network user using a transmitted identifier, in particular, the network address of the network user (1a, 1b, ..., 1e), and encrypts the time signal (5, 10) with a key generated by the assigned clock system (4a, 4b, ..., 4e) and/or with the identifier, and transmits it.

5. A method for transmitting data with a tamper-proof time stamp over a telecommunications network (2) from a first network user to a second network user,
wherein the data, along with a time signal obtained in accordance with a method as recited in one of the preceding claims, is transmitted from the first network user to the second network user directly or indirectly via the central system (3).

6. The method as recited in Claim 5,
wherein the data and/or the time signal is/are encrypted by the first network user (1a, 1b, ..., 1e) during transmission, especially with the key present at the central system (3) and at the first network user (1a, 1b, ..., 1e) and/or with an identifier of the first network user (1a, 1b, ..., 1c).

7. The method as recited in one of Claims 5 through 6,
wherein a central system (3) is provided at the second network user.

8. The method as recited in one of Claims 5 through 7,
wherein the central system (3) returns an acknowledgement of receipt, especially with a time signal (5, 10), to the first network user (1a, 1b, ..., 1e).

9. A system for generating a tamper-proof time stamp in network-based communication systems,
wherein the system includes a central system (3) and one each clock system (4a, 4b, ..., 4e, 6a, 6b, ..., 6e) on the side of a network user (1a, 1b, ..., 1e) and on the side of the central system (3); the clock systems (4a - 6a, 4b - 6b, ..., 4e - 6e) being assigned to each other and to the network user (1a, 1b, ...,1e) and operating synchronously to generate a key which changes, in particular, at intervals of time, and with which an, in particular, officially recognized time signal (5, 10) can be encrypted in the central system (3) and decrypted by the network user (1a, 1b, ..., 1e) after it is sent to this network user.

10. The system as recited in Claim 9,
wherein the central system (3) is formed by a time signal transmitter (5).